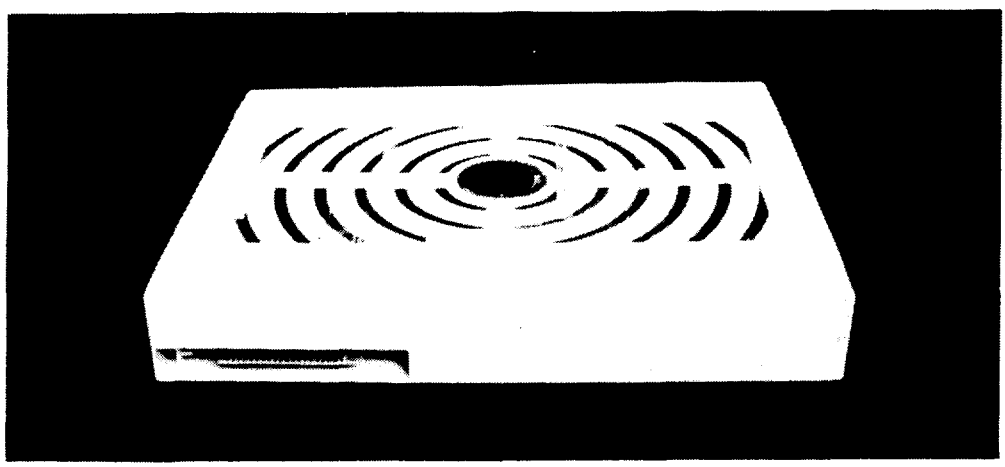
S.U.N. Is On The Horizon - What Will We See When It Shines?

by Karen JP Howes

Last fall, DECTEC International Inc. completed the design of a satellite scrambling system called the Secure Universal Norm (S.U.N.). The system makers claim it will provide the satellite industry with a highly secure and functionally unpiratable signal scrambling system, and they say it doesn't require dealers, TVRO owners or programmers to change anything that is already in place.

But can a small Canadian R & D firm change the way we have been taught to understand satellite scrambling?



The S.U.N. descrambler is enclosed in a white plastic case bearing its name on a gold emblem at top centre. The descrambler itself contains no descrambling processes. The S.U.N. unit receives its instructions from a "Super Smart Card" which is plugged into the slot at the front of the S.U.N. unit. Security information is hidden deep within the self encrypting processor carried in the "Super Smart Card"

An Acquaintance With Scrambling

Within the past six years, each of us to one degree or another has become pseudo crypto-ites. We casually toss around neat new words once only familiar to cryptologists and mathematicians. Ask anyone else to word associate with "movie" and they'll say "popcorn". But from our psyche comes quirky nomenclature like seed keys, algorithm, sync inversion and DES.

Still most of us actually know very little about encryption. We expect it to be like our television. Turn it on and it works. But the technology hasn't been so gracious. Industry trade reports over the years have shown that anywhere from two to three million of the 3.2 million Videocipher descramblers, manufactured by General Instrument Corporation for the North American home satellite market, function as pirate devices. Programmers have lost hundreds of millions of dollars in revenue and the growth of the Direct-To-Home (DTH) business has been stymied.

Two years ago, HBO and ESPN went so far as to form a joint venture to seek a new encryption system to replace Videocipher II and today most programmers either believe that GI's PLUS version or its upcoming RS module will provide a secure solution, or they have thrown up their hands in disgust and have decided to await digital compression.

The New Kid Moves In

But last November, a small Canadian research and development firm unveiled a revolutionary approach to satellite scrambling. The company's claim that they had developed a universal, open architecture scrambling system shocked even the most open-minded and drew pointed criticism from the skeptical.

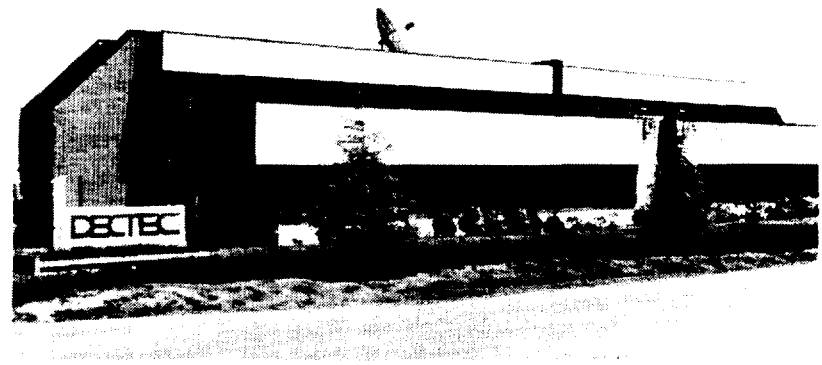
In a letter drafted by Taylor Howard, head of research and development for Chaparral and technical consultant to the SBCA's anti-piracy task force, the author insightfully noted that "it (the S.U.N. decoder) is a well done piece of printed circuit board work that used field programmable gate arrays (FPGA) technology to emulate the, up till now, proprietary chips which GI has used to control the patent and copyright technology."

"Emulate," Mr. Howard continues, "is an important word here because much heat will be generated over the possibility of emulating without infringing."

Still, the general consensus remained that DECTEC's technological breakthrough was not really possible. So if it wasn't possible, it must be a deceptive trick. That explanation satisfied many. But the question arose, how much can any of us really know of what is possible in a constantly evolving and changing world comprised of things too small to touch, let alone see and truly comprehend.

Smart Cards

Since before Sony developed Telefirst for ABC, scrambling systems have been designed as closed architecture networks. Their design requires the sys-



DECTEC's offices in Sidney, British Columbia

tem's functions to be hard wired into custom chips that are soldered into permanent board positions. This proprietary approach to product design functions such that when an encryption system provider sells his system to a user, the provider becomes the sole supplier of decoders and encoders for the life of the network. If the system is compromised, security can be restored only by replacing each subscriber's decoder. Also, if the network owner decides to upgrade or alter features within his own system - e.g. the number of "tiers" - he must again undergo a system-wide replacement.

Because systems are hard wired and difficult to upgrade or replace, the commercial encryption industry has not been motivated to keep encryption technology up-to-date. In fact, even the most recently announced systems: Videocipher II Plus, Prime Star's version of BMAC and the updated Leitch, are still based on the technology of their parents and are conventional and closed by design. Some of these systems have been updated though as they will soon employ a smart card in order to keep the decryption key out of the actual descrambler. While the smart card approach, originated in North America by DECTEC, allows the system operator to replace smart cards when the security portion of the system is compromised, the functions and features provided by each of the "new" conventional systems are inherently unyielding.

An open architecture approach is more elegant. It leaves nothing of consequence within the decoder itself. All processes, algorithms, functions and features of the system are provided through software. The software tells the decoder how to behave. Thus, the same decoder box can be programmed to decrypt several different encryption processes.

Specifically, the first release of the S.U.N. system comes equipped with enough memory to simultaneously process two or three different descrambling programs. For example, one program designed to configure the S.U.N. decoder to behave as a Videocipher II unit can run concurrently with a second program providing S.U.N. with the characteristics to act like an Oak box. The S.U.N. box is designed to identify the scrambled signals coming into the box and automatically switch between the software programs loaded within.

Once the S.U.N. box is configured in any specific way, the unit's owner can only access a scrambled signal if he subscribes to, pays for and is authorized to be turned on. Where the S.U.N. system again differs from the conventional design is that the authorization process is reconfigurable. In the current VCII environment, S.U.N. units loaded with the appropriate software could be authorized through one of several methods including: through G.I.'s own DBS authorization center; directly by the programmer through DECTEC's Universal Data Teleport or by way of a telephone line; or through smart card updates. (The latter works best for authorizing one time events distributed to a manageable number of receive sites).

Most surprising about the approach taken by DECTEC is that while DES systems like Videocipher require the same secret key to be used to both encrypt and decrypt data, S.U.N. is able to emulate the VCII system and provide authorization without the use of any of GI's seed keys.

John Grayson, CEO of DECTEC International Inc., explains that the Secure Universal Norm scrambling system is as different to conventional scrambling systems (like VCII, Oak, BMAC and Leitch) as algebra is different than geometry. While both are mathematics and either can be used to solve relational problems, the two are inherently different.

The Dawn Of SUN

DECTEC first departed from the conventional approach to scrambling three years ago during a preliminary planning session. "We were focused from day one", explains Mr. Grayson. "We weren't interested in offering just another scrambling system. We knew DBS was on its way and we understood what the DTH industry was going through. We wanted to develop a technology that would make it possible for the consumer to have one decoder in his home yet leave open the method and application of encryption and authentication on an ongoing basis."

So, sketched on a piece of company letterhead dusted by sand and cool Canadian sea air, Grayson wrote these notes: (1. compatible with Videocipher and Oak; capable of being configured to offer BMAC, (2. functionally unbreakable and (3. changeable.

A nice idea. But it didn't seem possible. That is, until one year later when a company out of San Jose unveiled new developments in gate array technology. Fascinating breakthroughs in field programmable gate arrays and, specifically, Logic Cell Arrays, brought Grayson back to his salt-washed notes. He then teamed up with a notable British scientist and began the arduous process of research and development which not only involved the blind-engineering of the Videocipher technology but also required DECTEC's engineers to push the design parameters of FPGAs.

Meanwhile, back in the civilized world we were becoming more and more acquainted with conventional scrambling. We were taught about encryption methods, the difference between hard and soft scrambling. We rehearsed which keys did what and we were beginning to get the gist of what it all meant. But still at the forefront was the damage created by piracy.

John Grayson, DECTEC International

Night Falls On Firmware

Essentially, scrambling eludes us because its physical presence is beyond our perception. The processes, features and functions of scrambling systems are based on mathematics. This is why DECTEC engineers were able to tap into the power of reprogrammable gate arrays to create the first universal scrambling system and enable what was once done in firmware to be provided through software.

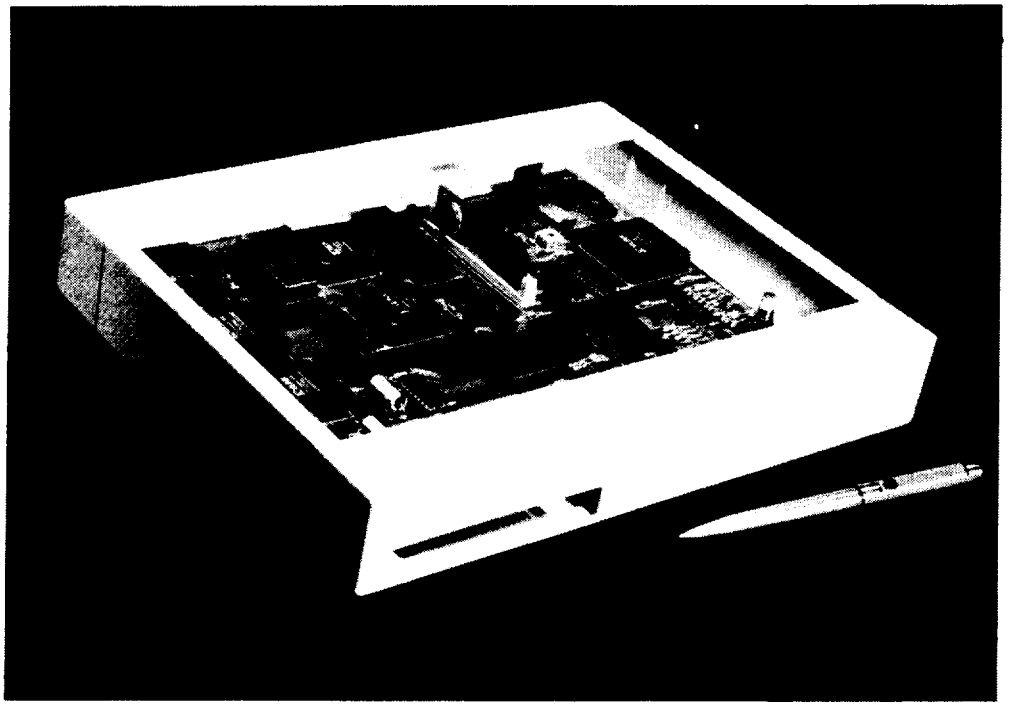
While this open architecture approach is dramatically different from what we have become acquainted with over the past six years, if it proves to offer greater security and more system flexibility - if it can allow several encryption systems to be processed through one piece of consumer hardware, and if it can offer choice and competition where none has previously been allowed to exist, then maybe some of us can forego yet another learning process and know simply that, when we turn it on, it will work, and that we won't have a pile of different decoder boxes stacked on top of our TVs.

In Summary

DECTEC's technological breakthrough was fundamentally designed to provide consumer, programmer and present or future scrambling makers with a universal platform through which competition and innovation would flourish.

"We realize that our S.U.N. system disrupts the status quo," explains Mr. Grayson, "so we plan to bring the Secure Universal Norm scrambling system to the DTH market as we brought its design from drawing board to finished product. We will proceed in an orderly and focused manner."

The Fundamentals of Signal Scrambling and How They Relate to S.U.N.



The Locks

Signal scrambling can be divided into two areas of discussion - 1. the method of scrambling/descrambling and encrypting/decrypting signals and 2. the method of managing, securing and communicating the information which enables the first step to occur.

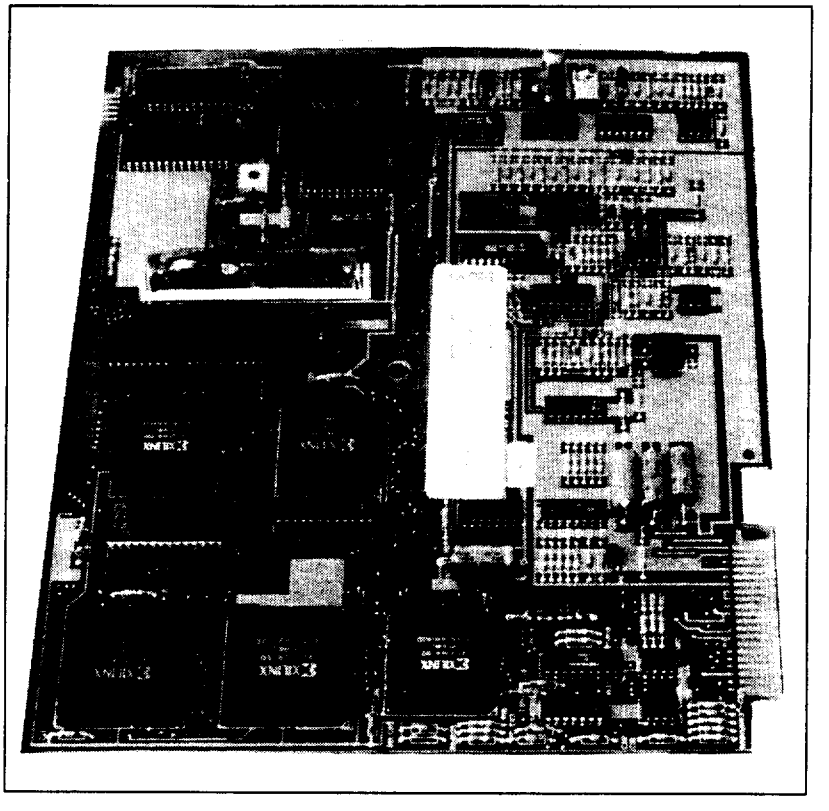
In the past we focused our attention on the first area, how to attain the most secure scrambling/descrambling procedure at the least cost. Initial experience showed us that some analog scrambling techniques were simple and inexpensive to crack.

Patrice Peyret, product development manager at Gemplus Card International Inc., says that most analog scrambling systems involving RF-level scrambling and sync modification are relatively insecure since any person with knowledge of frequency characteristics and equipped with receivers outfitted with sophisticated sync separation circuitry can easily display an undisturbed picture.

Oak Orion, for example, employs a video scrambling method which randomly alternates between various inversion modes. In the Videocipher II system, video information is inverted between sync pulses and then suppressed. According to Tom Shimabukoro, Director of systems planning and analysis for GTE's Spacenet and author of Securing the Corporate Village, Oak's video scrambling technique is more secure than VCII's.

Analog scrambling systems based on modifying the active part of the video signal, states Peyret, are more secure. The Line Cut and Rotate method used by both Videocrypt and Eurocrypt, and the popular Video Line Shuffling process used by Leitch both require the use of real time spectrum analysis to reverse the distorted condition. But the most secure form of scrambling, per se, is when a signal is processed digitally, sampled, then randomly intermixed.

The audio portions of VCII, Oak and BMAC and both video and audio signals within the Leitch commercial unit and VC I are hard scrambled - that is, the analog signal is converted into binary streams comprised of zeros and ones. Once digitized, the signal's sequence is mathematically manipulated (for example, run through a complicated algorithm like DES or any other polynomial). Conversion back to the analog format produces a distorted signal unless a decoder is given the key to reverse the original equation. This is why many now look forward to the sterile digitized environment of compression where we believe that the security of a digital systems is based on how "difficult" is the mathematical formula creating the cryptosystem.



It's the same premise that led VCII designers to first claim their system was unbreakable. And they were right if they considered the entire system to be the process of encrypting the audio signal through the DES algorithm.

Theoretically, the only way to break DES is to try every possible key to find which one transforms ciphered text into recognizable information. In the DES process, each key is 56 bits long, creating some 72 quadrillion possible keys. Even in using a high speed computer capable of running 10,000 DES operations per second, it would take 114,246 years to find 1 key. But who needs to sit at a computer for 100 centuries if the decryption key is accessible? The best lock (or algorithm) won't keep out trespassers if the key is always kept under the door mat. This realization is what has most recently turned our attention to the second area - the key management aspect of scrambling.

A sampling of existing descrambling products;
Top: Oak Orion - Middle: General Instrument VideoCipher II - Bottom: Leitch ViewGuard

The Keys

According to James Bidzos, president of RSA Security, "...the greatest weakness in any cryptosystem is the handling of keys." Insecure management of keys and access control systems is what enabled hackers to break Oak, VCII, and BMAC. It is also why PLUS is expected to be broken and why even digital compression is vulnerable to breaches in security. We now have at our disposal a host of reasonably unsolvable algorithms which have given us a secure lock. So we now move on to consider how we can best transport and store the key that opens the lock.

In the conventional approach, a handshake is required whereby the sender provides the receiver with a common key which is used to both encrypt and decrypt date. The common key is combined with another key which is embedded into the physical decoder. The fact that a key is put in one place is what makes a system penetrable.

The S.U.N. system, however, does not require a handshake and the control data is neither stationary nor accessible.

Through DECTEC's open architecture approach, the keys - which are replaceable and carried on a removable smart card - are themselves encrypted with a complex mathematical algorithm. It is the same system employed in Europe for electronic bank transfers. But the very nature of the logic-based, universal platform developed by DECTEC has provide the Secure Universal Norm with an additional and perhaps more deterring safeguard. Within S.U.N. not only can the keys be continually and randomly repositioned and replaced, but the lock can also be changed.

Because S.U.N. can be completely reconfigured in the field at any time, the entire digital processing scheme can be changed. Where both the keys and locks can be easily and cost effectively altered, the system becomes functionally unbreakable.

About the Author:

Karen JP Howes is a communications consultant based in Atlanta, Georgia. Karen has been writing for the satellite industry since 1984.

Pondering the Smart Card

TVRO Sets Its Mind on Secure Encryption

BY DAVID HARTSHORN

Just think about it: a cheap piece of credit-card-sized plastic that packs a microcomputer powerful enough to vex even the most savvy of pirates. If, perchance, hackers crack the system, the card can be replace within days, rendering chippers' efforts useless.

Still more thought provoking is the fact that the smart-card system is available, is proven and is fast becoming the encryption method of choice in European and North American satellite TV markets.

General Instrument (GI) calls it a CipherCard. Dectec, the controversial Canadian decoder manufacturer, opted for the Dallas Sip Stik and the British Sky Broadcasting (BSB), a U.K.-based direct-broadcast-satellite (DBS) concern, has dubbed it a Key Card. Satellite chippers call the emergence of such systems - more commonly known as smart cards - everything from a pain in the neck to the beginning of the end of the "good ole days" of the piracy underworld.

Where smart cards are concerned, the expression "precious things come in small packages" has never been more true. Indeed, not since the advent of microprocessors (an enabling technology of smart cards) has such a small, unassuming product packed so much punch. Smart cards are called "smart" by their creators because they contain a minuscule computer chip that enables the product to say one step ahead of the pirates.

For example: European telephone companies and banks pass them out to customers who then stick the cards into pay phones or 24-hour teller machines to make calls or withdraw money. Because the smart-card chip is packed with high-level security systems, criminal elements are hard pressed to "crack" the system and fool it into diverting funds or services to unauthorized users.

But even if pirates find a way to break into the smart card (and herein lies the rub), the company can simply issue customers a new one - at very low expense - with a brand new security system that sends pirates back to the drawing board. This scenario can be repeated indefinitely, rendering piracy a most unappealing vocation.

The implications for the TVRO industry are enormous. The decoding system in the U.S. - GI's VideoCipher (VC) technology - not only is bulky and expensive, but it also has been proven to be more user friendly to pirates than it is to legal customers. GI is reminded daily of this fact by an irate TVRO industry, and the company is moving to adopt a smart-card-based system.

Likewise, GI's competitors, including Dectec and Scientific-Atlanta (S-A), supplier of the encryption system for PrimeStar's DBS service, are seizing upon smart cards as the ultimate weapon in the fight against signal pirates- and in the battle for market share. They have high hopes for the system and rightly so. Customers of their U.K. counterpart, BSB, have been using the smart card since the British service's inception two years ago and it has out-performed expectations.

In short, smart cards may provide the ailing U.S. TVRO industry with the security it needs to move beyond offering a hacked service to limited markets. With smart cards, the TVRO industry can seek out a secure, profitable business that reaches into the living room (and pocketbook) of every American.

Us vs. Them

So why haven't smart cards already taken hold in the U.S.?

"Nobody knows," laughed Stephan Seidman, editor of *Smart Card Monthly*. He said the technology's arrival has been delayed by U.S. market "peculiarities," such as the TVRO industry's heavy dependence on one decoding module brand. But Seidman predicted that it's only a matter of time before smart cards take off. Momentum is building elsewhere in the world, where more than 100 million smart cards already are used in applications that range from satellite TV to banking, from pay-phone cards to high-level security.

The technology is uncrackable so far, with the emphasis on "so far."

The technology is uncrackable so far, with the emphasis on "so far," Seidman allowed. MasterCard put several top hacks on the technology, daring them to crack it; they were stumped. Similarly, a British security agency sanctioned noted members of the pirate underworld to break into the smart card and they too ran up against a wall ... or, to be more exact, walls.

Seidman explained that many smart cards pack a "bag of tricks," each one of which triggers the card's shutdown when someone tries to crack it. If hackers use a wrong access code more than three times, the card goes dead. It it's opened, it goes dead. If the device is scanned with an electron microscope, hitting the card's sensing cells, it goes dead. And so on.

Such innovations have been around since the 1970s, when the French first cashed in at the patent office with the idea of integrating a secure chip on a card. Since then they have dominated the field, establishing footholds in continental Europe, the U.K. and, more

recently, the US. But some key patents are running out now and Seidman predicted that as French licensing power diminishes, cards will get even cheaper.

In the meantime, several companies have positioned themselves in the U.S. for a smart-card business boom that has been a longer time coming than had been projected. Consequently, key smart-card manufacturers in the U.S. have scaled back operations, said Joseph Schuler, president of Gemplus Card International (GCI), a major French smart-card manufacturer involved in the U.S. market. The company, with an office in Rockville, MD., nonetheless is poised to add to the tally of smart cards it has supplied to various vendors — 50 million since 1988. He agreed with Seidman, calling smart-card companies' downsizing an "adjustment" to a slow-moving U.S. market.

Thinking European

One of the first to successfully implement the smart-card design in a satellite system was BSB, a DBS operator formed last spring when two competing services, British Satellite Broadcasting and Rupert Murdoch-owned Sky Channel, merged. It has sold close to two million systems in two years and has sold 60,000 more units per month since June, according to an independent consumer survey conducted by the *Financial Times* of London.

While the company is paying dearly to stay in the game – $1 million per week in losses are being added to its $300-million debt – BSB's service is growing in popularity and is expected to begin recouping losses in 1992.

For less than $350 BSB customers receive 48 Ku-band channels and a system that consists of a 60-cm dish (about two feet wide), an LNB and a receiver with a built-in smart-card system called Videocrypt. At the system's heart is the Key Card.

"It has yet to be cracked. But I'm touching wood," said Gwynn Morgan, communications development manager of Jerusalem-based News Datacom (ND), which is partially owned by BSB and helped develop the company's smart-card system. He said it works so well that the BBC has adopted it for use in a planned terrestrial TV niche market service that will involve downloading transmissions to VCRs. Other Videocrypt users include: Spanish broadcaster Retevision; New Zealand's Sky Network system (unrelated to BSB); Palapa's pan-Asian satellite TV network, and two more broadcasters are expected to sign contracts by late this month, "one in the U.K., one in the Southern Hemisphere," said Morgan.

Morgan said the approach behind BSB's smart card diverges from the classical encryption approach in which keys are used: "Our approach is rules-based." Morgan compared the classical approach - building a series of keys - to locking a diamond in a safe, then putting that safe inside another safe and so on. "The trouble there is if the hacker finds just one of the keys he can find a way in."

By contrast, ND's approach, called the one-way process, is like trying to get in a nightclub: "I walk up to the door and knock three times and ask for Harry. But tomorrow I have to knock four times and say, 'Julie sent me.' You change the rules."

Morgan said BSB's smart-card rules are changed approximately every six months, which makes it "virtually impossible" for a pirate to make money. Morgan added that the code used to be changed every three months. But there was no indication that hackers were cracking the system, so the frequency of smart-card changeouts was reduced.

Cognitive Dissonance

BSB's major contender in the European smart-card market is Eurocrypt, a system developed by a joint venture consisting of a "who's who" of electronics manufacturing, including Bull, Nokia, Philips and Thompson.

Eurocrypt is gaining ground, too. It's used in Scandinavia through the programming services of Scansat. In addition, TV3 in Denmark, Norway and Sweden and TV1000 are planning full use of the system. In France, services from TDF-1 & 2 use Eurocrypt to control access to premium programming of Canal Plus, the French broadcasting system. Also in France, users on cable nets in Paris and in other cities get premium programs through smart card-based decoders supplied by France Telecom.

The Eurocrypt system works like this. Over-air messages are sent to an address in the smart card, which is inserted in a decoder. The messages tell the smart card which program or other services it may allow the decoder to descramble. Such messages, sent regularly to maintain authorization, are generated by a subscriber authorization system that can act independently for different operators.

The smart card is divided into zones, each of which controls the entitlement of a programmer or group of programmers. It is thus possible for the user to have access to competing services or programs authorized from different countries through one card issued through a central location. The information can thereafter be updated via satellite transmissions.

"Before the smart card, everyone in the subscription-TV business had a nightmare that they were running a department store with no cash registers. That's behind us now."

Eurocrypt's owners have allied their system with the D2-MAC color TV transmission system to offer a package that they are urging the European Community (EC) to adopt as the encryption/transmission standard for the EC member countries. PAL is currently Western Europe's closest thing to a TV standard (France uses Secam). But the European receiver manufacturing sector wants the MAC/Eurocrypt team adopted as the European standard.

BSB spokesperson Jonathan Miller said both systems probably will "do the job," but what's important is that the winner be decided through marketplace competition. While both camps are

waging all-out war, there is at least one point of agreement: Smart cards make it possible to refresh the security system. So the European satellite-TV industry doesn't find itself in the same position as its North American cousins, who have been unable to "leapfrog over the pirates."

Miller said the same won't happen with smart cards, because they act as the subscription-TV equivalent of a nuclear deterrent. "The mere threat that you can quickly renew the security is enough to deter pirates.

"We will not build a business assuming that no one can break the smart card."

Before the smart card, everyone in the subscription-TV business had a nightmare that they were running a department store with no cash registers. That's behind us now."

Wising Up

The U.S. satellite TV industry may be tainted, but it's still arguably the most lucrative potential consumer market in the world. Thus, major forces – hailing both from Europe and the Americas – have arrayed themselves to take advantage of the potential explosion in smart-card demand. **Not only are companies like Dectec, GI and PrimeStar poised to seize the moment, but also component manufacturers like Dallas Semiconductor (DS), GCI and S-A.**

S-A, in particular, has been fast off the mark, albeit on a small scale. It's been supplying smart cards to PrimeStar since early 1991 in conjunction with PrimeStar's national DBS rollout to test markets. The cards work with the PrimeStar Model 9706 IRD, which the company has been shipping for nine months.

"We'll use [the smart card] as an integral part of up to four products," said Dwight Duke, vice president and general manager of S-A's digital video systems division. Based on how the product evolves, the company plans to integrate it into all its satellite products, including the Model 9708 business TV receiver, the PrimeStar unit and international products "soon to be announced."

GI meanwhile, plans to introduce CipherCard as the smart-card component of its next-generation VC II Plus RS (Renewable Security) descramblers. But CipherCard won't be "invoked," a GI spokesman said, until a security breach forces programmers to request a security upgrade to CipherCard. Until such an upgrade is necessary, RS modules will function identically to VC II Plus units.

GI's smart card will be slightly thicker than a credit card, because it will have a high-powered battery and large microprocessor. "We use the smart card as a launching point," said Michael Meltzer, GI's vice president of marketing. He explained that GI plans to take a smart card and endow it with a custom-tailored die.

As of late September, GI was performing in-house analysis - or alpha testing - of the RS unit. Beta tests, which involve gathering feedback from OEM's, distributors and dealers, were scheduled for early October. GI plans to begin manufacturing RS decoders after beta testing in late December.

"That allows for a beta test that may or may not come back 100 percent," Meltzer said. "We can make some tweaks if we find a minor bug. If we find a major bug, it could put the [manufacturing] schedule at risk." Provided there are no problems, Meltzer said, it will be April before GI reaches full RS production.

As for GI's smart-card chip, the company has joined a long list of clients of GCI, including BSB and Canal Plus. GCI formed in 1988 by a team of SGS-Thomson executives, is an international integrated-circuit manufacturer based in Gemenos, France. It has been providing chips for GI's smart-card test program, said Schuler.

A GI spokesman confirmed it's using Gemplus equipment in beta testing, but he said it's also working with several other vendors of smart-card components in the program's development stage.

All told, GI is analyzing 25 vendor's components for possible use in the CipherCard. Meltzer said GI didn't yet know the CipherCard cost, but Schuler said a "very sophisticated" smart card manufacturing in volumes of 100,000 would be in the "high eight dollar [per unit] range"; at 500,000 units, the cost per unit would drop to "low eight dollars"; and orders of one million would be in the "seven dollar range."

Consumers will see RS modules beginning in the first quarter of 1992. But the end user won't see the CipherCard until or unless the RS unit is cracked. "We will not build a business assuming that no one can break the smart card," Meltzer said. "It may be that no one does. But we have to assume it will happen and build a program for that contingency."

Canadian Brains

Dectec, GI's controversial Canadian competitor, has plans of its own. Dectec president John Grayson already has signed a contract with a smart-card supplier, Texas-based Dallas Semiconductor (DS). While Dectec's decoder, called the Secure Universal Norm (SUN) now uses a plug-in "smart chip", next-generation SUN models, scheduled to appear in early 1992, will have a smart card.

Grayson told TVRO Dealer that he is showing programmers the smart-card version. It incorporates the same microprocessor but can plug in sideways instead of having to stand on the board. Grayson said Dectec's cost per smart card is $22.50 in quantities of 100,000 units; in quantities of 250,000, the cost drops to $15.

As of late September, samples already had been delivered to Dectec and production was set to begin by early November, said DS area manager Tom Hunt. His company, which manufactures semiconductors and smart cards, has been working with Dectec for 18 months and will manufacture the card for use in SUN. Dectec, not unlike GI, will customize the card with proprietary software.

"Our card and microprocessor take many man years to crack," Hunt said. "Our patents are based on encrypting data and the program, so Dectec can put

both inside the card and no one else can get in and see what has been done."

Hunt predicted the smart-card business would grow by 25 percent per year for the next three to four years, compared with flat sales in recent months. Growth will be driven by a combination of demand from satellite and other consumer electronics industries, which he predicted will generate demand for "astronomical quantities".

DS is a seven-year-old company that concentrates on OEM business. Hunt said DS is "talking" with other satellite companies, but deals haven't been signed. The company also sells to heavy hitters in the computer business, including IBM and Compaq.

Grayson said comparing Dectec with others in the satellite industry is like comparing a pocket calculator with a home computer. "The home computer can be upgraded and can use different software packages." The component that enables such an approach is called a re-programmable gate array, and is manufactured by Xilinx, San Jose, Calif. "They contain nothing," Grayson said. "You can ... program them to become any custom chip you want. The consumer switches to VideoCipher or to an Oak signal automatically."

Meanwhile, Grayson said he is "anxiously awaiting" the introduction of GI's RS unit to see if the company has "stolen" Dectec's technology. Grayson's comment was a reference to GI's raid several months ago on Dectec's headquarters in Sidney, British Columbia. Acting under authority of the Anton Pillar provision of Canadian law, GI seized materials and information on the Dectec system.

GI said it was seeking to prove that Dectec was manufacturing equipment that illegally incorporated proprietary GI technology. Since then, however, GI hasn't deactivated SUN units using electronic counter measures (ECMs) which some analysts say is evidence that GI hasn't been able to crack Dectec's smart system. Hunt, whose technology is used in the equipment, said he was "amused and pleased" to see the system still operating, despite GI's seizure of Dectec blueprints.

How Smart Is Smart?

Never say "never" is the rule when it comes to assessing an encryption system's invincibility. While it isn't economically viable to hack smart-card technology, the use of such technology doesn't "confer immunity" to hacking upon a system, according to John McCormac, co-author of *World Satellite TV and Scrambling Methods* (Baylin Publications). McCormac, a noted U.K. hacker, said there always will be encryption loopholes that can be exploited.

For example, BSB's Videocrypt system has been "theoretically hacked" using what he refers to as – by no coincidence – the "McCormac Hack." While acknowledging that Videocrypt can be reconfigured, he said the approach can be applied at different points in the descrambler. But the prime requirement is a datastream that can be extracted and used to activate other decoders.

A system that has a "frozen architecture" – one that has been implemented in application-specific integrated circuits – eventually will be hacked, McCormac said. Some authorities mistakenly consider it a defense that the key sets in a frozen architecture system can be re-programmed, he said.

If certain hacks are running on a system, clones simultaneously will receive the new key sets, and the "stagnant" architecture makes it difficult to implement countermeasures. The only defense against this type of hacking is a secured datastream architecture and an "agile" system. The smart card is a step in the right direction. But he said the only North American design that has been reported to meet the criteria for a truly open-system architecture is Dectec's SUN decoder.

Never say "never" is the rule when it comes to assessing an encryption system's invincibility.

Be that as it may, all smart-card-based systems, whether planned or in operation, are based on the premise that they soon will be or already have been cracked and thus must be changed out regularly. Faced with a technological landscape of ever-changing smart cards, the replaceable technology will drive profit-minded signal pirates from the business.

That's the theory. How it holds up against the best efforts of an international community of hackers will determine whether the satellite TV industry will be forced yet again to conjure new decoding alternatives or be left to thrive on the thought that pirates' ranks have been reduced to hackers who hack for hacking's sake. **TVRO**

InRoads to hi — technologies

February 1992 The journal of entrepreneurism and innovation in hi-tech industries.

ENTREPRENEURISM

- **Entrepreneurism**

"A Better Mousetrap Isn't Enough" ..... 1.

"DECTEC Wins Round in Multi-million dollar Patent battle" ..... 3.

"DECTEC Scrambling System -- Good for the industry, is the industry up to it?"..... 4.

"Night Falls on Firmware" ... 7.

- **Innovations**

"Skypix/Mitsubishi set sights on April Launch" ..... 8.

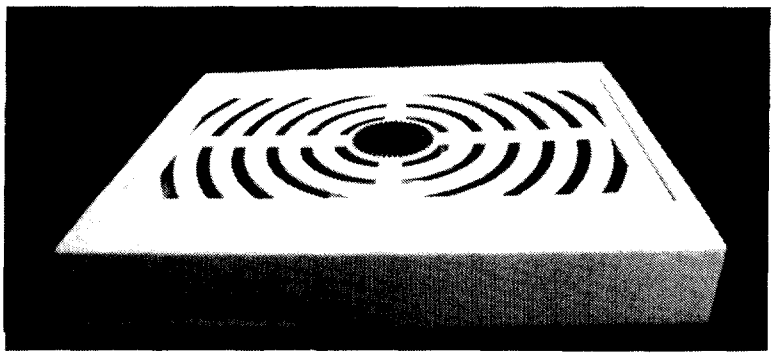
"DirecTV: Thompson/Hughes reach for Sky Cable"..... 9.

"Engineers research new mixed-media satellite video services" ..... 9.

- **Analysis**

"Compressed Digital Broadcast Video Technology: adoption potential among business television networks"..... 11.

DECTEC's innovative flexible scrambler is shut out of North American home satellite marketplace. Company wins latest legal skirmish, but is hit hard in market by GI and cable monopolies. Company discusses strategies and plans.



DECTEC's multiformat flexible S.U.N. scrambling system originally designed to provide competition in the North American TVRO and Cable marketplace is turning to other applications. CEO says pay-tv market in U.S., Canada does not offer level playing field.

Better Mousetrap Isn't Enough to Get into TVRO/Cable Market

Imagine you're the head of a small high tech company. You have a creative team, a good idea, and a research facility comfortably situated between mountain and sea on the western coast of British Columbia. Financed by personal savings and scattered research grants, you go to

work.

Three years later, your forward thinking staff turns out an impressive consumer electronics product. It's a multiformat scrambling system for satellite and cable systems. It's the first consumer electronics product that can be reprogrammed within a person's home by using the same type of smart cards as is used in electronic banking machines.

Best of all, your product is generations ahead of its predecessors, and it will reduce the cost of a consumer satellite receiver from $1100 to $300. This will bring the cost of a $1500 satellite system down to $700 and create competition for cable operators who will be forced to drop cable rates in order to keep customers. What a goldmine!

Wait. Stop. It means you have to compete against a company that holds a monopoly on decoders in the home satellite market. But what do you know about how a $1.6 billion monopoly would react to a little bit of competition? So, you put out a press release. And less than three months later your competitor raids your research labs, empties your notebooks, copies your data files, downloads your trade secrets, and walks out of **your** offices with nearly half a million dollars of **your** inventory. But they give you back something in return.

They leave you with the biggest stack of paper you'd ever seen in your life. Your attorney says its a lawsuit claiming you infringed your competitors patents and copyrights. And by the way, your attorney also says that the raid was perfectly legal. It was a court issued "Anton Pillar" Order usually granted by Canadian courts to provide for the preservation of evidence.

This is not a trick question: What do you do? Most companies would write a letter of apology and say they would find something else to make. But from a window view of the Saanich Inlet off Vancouver Island, the CEO of DECTEC International Inc. paused briefly while patent experts analyzed the claims against him. With expert opinions in hand, DECTEC's John Grayson quite publically announced that his company didn't copy anybody's patents and he was going to sell his decoder, anyway.

DECTEC then drew up a counterclaim against their San Diego based competitors, General Instrument and publically traded Titan Corporation (NYSE;TTN), initially asking for $20 million dollars and charging the companies with stealing trade secrets. Mr Grayson also wrote a letter to the Canadian Prime Minister asking him why Canada has a law on its books which allows companies the right to search and seize materials from other companies, most especially competitors.

"our competitor has employed levels of industrial espionage unfamiliar to small companies."

-- DECTEC CEO, John Grayson

The question has gotten some Canadian lawmakers thinking. In a letter written to Justice Minister Kim Campbell, Member of Parliament Howard D. McCurdy referenced DECTEC's situation in asking the Minister to look into other ways to prevent the destruction of evidence.

But Mr Grayson says that General Instrument has manipulated more than the Canadian Judicial system. In a letter written to Prime Minister Mulroney, Mr Grayson writes, "our competitor has employed levels of industrial espionage unfamiliar to small companies in Canada." He goes on to describe how GI attempted to intefere with a grant DECTEC received from the Canadian National Research Council, and how GI encouraged the Canadian Department of Communications to publish a government booklet endorsing GI's decoder at DECTEC's expense.

Since General Instrument, Titan Corp, First

Choice Canadian Communications, and Cable/Home Corp filed charges against DETCEC in Canadian Federal Court on January 21, 1991, the matter has raised issues about how big companies can beat out littlier ones just by filing a lawsuit. For the giants it's a simple numbers game. If it costs GI $5 million to tie DECTEC up in court for five years, that's substanially less than the $60 million they'd give up in sales if DECTEC took just 10% of GI's market per year for the same period. So for the big guy playing Goliath, the object is to stall and spend money. David, on the other hand, has to fight the battle from a different ground.

Where GI uses teams of lawyers, private investigators and public relations muscle, DECTEC hired one lone attorney in Toronto, and a communications consultant in Atlanta. According to DECTEC's consultant, Karen JP Howes, "David can win against Goliath, eventually. The trick is staying solvent long enough to see the thing through, which means you can't play it their way. If you follow their lead, you're playing their game; and they'll win simply by changing the rules. We have our own strategies, and our own advantages -- chief among them is we're right; they're wrong, and sooner or later they'll make one too many mistakes."

Scoring one point for the underdog, DECTEC's legal counsel, Ian Angus discovered through depositions taken of GI employees that GI and the law firm of Stikeman and Elliott had violated court orders by releasing from protective custody the proprietary data taken from DECTEC's labs during the execution of the Anton Pillar Order. Under four separate court orders, the materials and intellectual property taken during the raid were to be protected and not copied or distributed to anyone, including to GI and Titan Corp. On February 3, Justice Teitlebaum issued a Show Cause Order asking GI and its lawyers to show why the court should not find them in contempt.

But the court battle isn't DECTEC's biggest problem. The company isn't able to get their product into the marketplace. "The consumer wants our product. The retailers want it. The distributors want it. But programmers like CNN are saying that they will only allow their channel to be seen by people who buy a GI decoder," explains Mr. Grayson.

"Imagine if you rented a movie produced by Columbia Pictures and were told you had to play it on a Sony VCR, or if you wanted to receive long distance telephone calls over AT&T and you were told that you had to buy a Mitsubishi telephone," explains Ms. Howes. "GI and the programmers appear to be dictating what

DECTEC Wins Round in Patent Legal Battle; GI may have Breached Court Orders says Judge

February 3, 1992; Canadian Federal Justice Mr. Honourable Teitlebaum issued a Show Cause Order requesting General Instrument and Its law firm, Stikeman and Elliott, to give reason as to why the court should not find the companies in contempt of court.

In the Show Cause motion filed with the court, DECTEC says GI, its attorneys and others defied 4 court orders protecting DECTEC's intellectual property by copying and distributing proprietary materials and trade secrets seized during an Anton Pillar raid on DECTEC premises last year.

The motion says that during execution of the Anton Pillar Order, GI and its attorneys added data files to DECTEC's computers, did not make complete lists of materials taken, and erased some of DECTEC's research files.

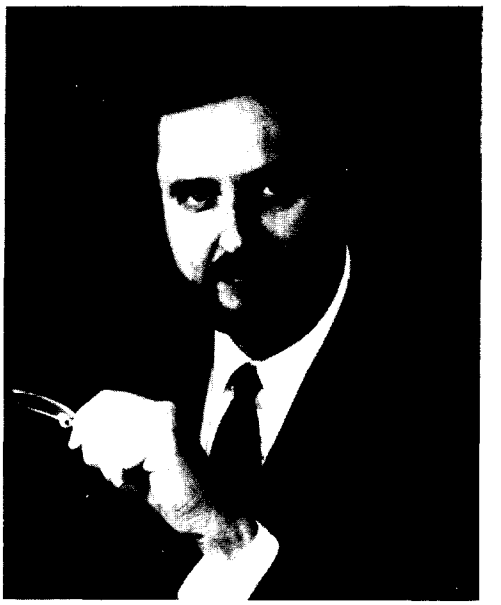
"Contempt of court is a quasi-criminal offense," says DECTEC lawyer Ian Angus. The Judge provided DECTEC with authority to subpoena top officials of General Instrument, Titan Corp, First Choice Canadian Communications, Cable/Home Corp and Stikeman and Eilliott.

hardware the consumer must buy in order to pay-for and access services openly marketed to satellite and cable consumers. It's like a record company telling consumers which CD player to buy. It's unheard of. But that's what's happening."

In response, the Consumer Satellite Coalition, which represents 2.5 million dish owners, asked the Federal Communications Commission in July of 1991 to hold hearings in order to "remove General Instrument's monopoly status" and encourage competition in descrambling equipment. Don Herron, executive director of the consumer group, believes programmers support GI because some of them may have been getting kickbacks.

But an even more compelling reason for excluding companies like DECTEC, says Mr Herron, is that "GI is the cable industry's leading supplier of convertors, and programmers either own cable systems or they are owned by cable operators. If they were to encourage competition and fair pricing for satellite decoders and programming, the price of a home satellite system would be about $750 and pay television would cost half what it does on cable." If that was the case, consumers might cancel their cable and buy a dish. So Grayson's technological dream come true turns out to be a marketing nightmare.

Faced then with a multi-million dollar legal battle and an anticompetitive marketplace, there may be no place left for DECTEC to go, but Grayson isn't waving the white flag just yet. "We have little hope for the North American market," says DECTEC's CEO, "But our Secure Universal Norm (S.U.N.) system has a future in other product applications."



DECTEC CEO, John Grayson, spent his years prior to hi-tech R&D as a recognized author and new music researcher. He is also considered a world authority on Sound Sculpture.

While DECTEC gears up for these new applications, Grayson says he has many legal options left in the U.S. and Canada. One of those options does not include giving in to GI, he says. "This suit isn't about patents," explains Ms Howes. "If it was, the two companies would be able to reach some kind of settlement. This is a spite case. GI wants to punish DECTEC and put them out of business. DECTEC's only option, here, is to win."

DECTEC's
S.U.N Scrambling System

Good for the industry, but is the industry up to it?

Let's say you are a research and development firm and you want to design a stand alone encryption system that you can sell to the TVRO, commercial, and other new markets, but you know that it will be too costly and inefficient to come out and ask programmers to spend a ton of money on new encryption hardware. What do you do?

In reality, this "hypothetical" scenario was what the Canadian based research and development firm, DECTEC International, was faced with when it began developing just such a system. Dectec's answer to the question of "What to do?", was to build a system that would be compatible with the current system(s), such as VCII and Oak, that could also act as a stand alone encryption system capable of running its own encryption/decryption scheme, and would successfully address many of the related signal "problems" that the satellite industry in North America is currently saddled with, including: security, expandability, and cost efficiency. The result? The Secure Universal Norm (SUN) scrambling system.

Dectec consultant Karen JP Howes compared the SUN system to a computer system that is easily upgradeable through different software applications. "It is a great deal more flexible than the current Videocipher system in that it is completely reconfigurable and field upgradeable" says Howes. Howes added that the reconfigurability of the SUN system gives it the potential to support video compression and thus, High Definition Television (HDTV).

The SUN system revolves around state of the art "smart card" technology and a renewable security (RS) module. The module can be configured to accommodate most any software application. In the unlikely event that the smart card's security is broken, a programmer could simply issue customers a new card, virtually overnight and at a very low cost, and the system is secure once again. Smart cards are already being used extensively throughout Europe, and their security thus far, has yet to be breached. Pirates beware!

The "smart card" contains a microchip which is located with some pretty hi-tech security schemes, as well as all the pertinent signal information necessary to decrypt the incoming signal.

Dectec estimates the cost of its module, to the distributor, to be around $100 once full production levels are reached.

The "brain" of the system, the smart card tells the RS module what to do. Once subscribers have their SUN module, they pay for the card according to what programming services they seek. The card is then loaded with the pertinent information and is shipped "authorization ready" to the consumer who merely plugs the card into a receptacle at the back of the receiver. (Current SUN modules require the customer to snap a "smart card" approach). The customer then turns on their equipment to find all the programming they paid for immediately available.

Programmers using the SUN system could each have their own authorization algorithm and access control system, essentially making them independent networks, and freeing them from the monthly DBS authorization center fees they now pay. But most importantly, the SUN system would offer them what they have, seemingly, wanted all along: 100% of the existing satellite receivers to be "legitimized".

Manufacturers should find the lower cost of the SUN module to be particularly attractive. Dectec estimates the cost of its module, to the distributor, to be around $100 once full production levels are reached. Quite a reduction from the $325 manufacturers currently pay for the Videocipher II Plus module.

The TVRO dealer base should be very interested in the SUN decoder because all of the decoder parts are off-the-shelf so the units can be repaired cost-effectively in the field by competent technicians. Additionally, distributor agreements are non-exclusive, as are service and repair contracts which are available to companies

that meet certain specified technical requirements. By contrast, GI's videocipher modules are only swappable by GI authorized dealers, and GI, at last look, hadn't authorized anyone to repair their VCII and VCII Plus modules.

A secure and upgradeable subscriber base could go a long way toward improved consumer confidence, which should, in turn, stimulate our industry. Even if the smart card were to be pirated, the convenience of only having to replace the card, rather than the entire module, would be a significant improvement.

The security aspect of the system alone, should give it tremendous potential in North America. With estimates of the number of illegal VCII's as high as 80% in the U.S. and 100% in Canada, one would think that the U.S. marketplace would be jumping for joy at the promise of such a system. But, our industry has a history of moving in unexpected directions.

Dectec has run right smack into General Instruments front yard saying "Hey, we have a better system. It's secure, less expensive, renewable, it utilizes state of the art technology, and is backward compatible with VCII. We've developed a swap out scheme that won't offend satellite customers and it's available today. Come and get it!" That is a great deal for the industry as a whole to swallow, let alone General Instruments.

General Instruments has retaliated with a lawsuit in Canadian Federal Court that could severely hamper Dectec's efforts at introducing its new system into the U.S. marketplace. The GI lawsuit claims that the Dectec system infringes on its patents and copyrights. GI announced earlier this year that it had succeeded in breaking through SUN's security.

In answer to GI's lawsuit, Dectec President, John Grayson has said that contrary to GI's announcement, the security of the SUN system has not been compromised, offering up sworn testimony by a GI official as evidence. Additionally, industry observers say that the fact that GI has not deactivated any SUN modules through the use of ECM's (electronic counter measures), lends credence to Grayson's statement that GI in fact has not penetrated any of the proprietary codes within the system. Grayson has also stated that the SUN system does not in any way infringe on any of GI's patents of copyrights.

DECTEC has filed a countersuit against GI which asks for $20 million in damages for alledgedly stealing trade secrets. Grayson apparently feels that the renewable security system that GI expects to introduce in early 1992, could really be DECTEC's. Reportedly, he is anxious for its introduction so he can see if his suspicions are correct. Both cases are pending in Canadian Federal Court, and it could be up to two years before they are settled.

The controversy surrounding the lawsuit could be the main reason why DECTEC has had difficulty in gaining support from any major programming entity in the U.S. While it has been reported that contracts between Dectec distributors and U.S. programmers have been signed, the names of those companies have not been disclosed. Likewise, the names of Dectec's Canadian distributors are also being withheld.

DECTEC has applied for executive membership in the SBCA, and has formally requested to become an active participant in and member of the Anti-Piracy Task Force, the SBCA Encryption Committee, and the Marketing Committee. But even here, the company has run into a snag. Because some SBCA members have questioned the prudence of allowing DECTEC to become a member, in light of the allegations surrounding the SUN system, the SBCA has referred the application to its ethics committee for review. As of press time, the committee had not rendered its decision. It is a delay for sure, but it would be hard to think that the ethics committee could

deny DECTEC entry into the association based on allegations. The committee's decision is expected sometime in December.

In our perspective, the SUN system represents the missing link in the encryption segment of the satellite industry; competition. Without competition the industry is robbed of a vital ingredient necessary to its well-being and continued growth. That ingredient is choice. Programmers, manufacturers, dealers, and consumers, for years, have been yearning for the option that the SUN system offers. To dismiss the opportunity that presents itself today, and others like it tomorrow, on the basis of allegation or misunderstanding would be a severe blow not just to one company, but to the entire satellite industry and all those who benefit from it, including customers.

This article was contributed by Heifner Communications Inc. which is a leader in providing satellite communications services and technologies for educational and private network users. Heifner provides programming to the private and wireless cable industries, and designs peripheral applications equipment for schools and universities linked via satellite. Heifner is located in Columbia, MO. at (314)445-6163.

Night Falls on firmware with dawn of S.U.N.'s reprogrammable software

Essentially, scrambling eludes us because it's physical presence is beyond our perception. The processes, features and functions of scrambling systems are based on mathematics. This is why DECTEC engineers were able to tap into the power of reprogrammable gate arrays to create the first universal scrambling system and enable what was once done in firmware to be provided through software.

DECTEC's Secure Universal Norm (S.U.N.) scrambling system takes an open architecture approach, which its designers say is more elegant than the hardwired conventional method. Founded on smart card technology, nothing of consequence is left within the S.U.N. module itself. All processes, algorithms, functions, and features of the system are provided through software programmed into a self-encrypting microprocessor carried on a smart chip or smart card.

The software tells the decoder how to behave. Thus, the same decoder box can be used to decrypt several different encryption processes. Once the S.U.N. decoder is configured in any specific way, the unit's owner can only access a scrambled signal if he subscribes to, pays for and is authorized to be turned on.

Another area where S.U.N. differs from conventional systems is that the authorization process is re-configurable and is based on software rather than on hardware. This gives programmers ultimate flexibility in changing control access functions such as key words and algorithms thereby enhancing the security within the scrambling system.

DECTEC International Inc is located in Sidney, British Columbia, Canada at (604)655-4463.

SkyPix/Mitsubishi Set Sights on April Launch

To many retailers and satellite installation experts, the re-appearance of SkyPix at the winter CES was a reminder that the system did not launch commercially last summer, as promised previously at the Winter 1991 Consumer Electronics Show. But, with the technical revising of the SkyPix system, and the arrival of Mitsubishi as a manufacturing knight in shining armor has come a major revamping of the home satellite receiver system itself.

Indeed, the revised Mitsubishi set-top digital video decoder and satellite data portal may be the architectural model of what the Cable TV industry, and many broadcasters perceive is their own individual corporate manifest destiny in the '90's: a digitally secure, digitally delivered home entertainment and multimedia center.

Another way of looking at the cumulative effect of the changes Mitsubishi has brought to bear on its commitment to the Kent, WA company: the revamped SkyPix receiver may just be the most powerful multimedia delivery vehicle ever to park atop a consumer TV set. New digital audio output ports and a high-speed data port may allow the under $800 system to deliver more then just Sky picks of programming: interactive games, TV programs, automated bill payment and more whiz-bang features may be part and parcel of its anticiapted April consumer launch.

But, there is a critical programming support mass needed to get any new DBS effort off the ground, and SkyPix may be the closest company yet to survive the barriers - spoken and unspoken - hoisted by a slew of programming-based rival video delivery industries whose existing program delivery monopolies perceive to be threatened by SkyPix's imminent consumer retail success.

SkyPix has used the Mitsubishi receiver redesign to allow the inclusion of several new consumer entertainment and interactive features, which will allow buyers to think they are getting "more than just another" cable box or video game. Among the major revisions are a Super VHS Output: SkyPix will deliver better than NTSC broadcast resolution to S-video VCRs and TV sets. A new CD-audio quality port will feature DAT Digital Audio Output. The revised Mitsubishi SkyPix box now delivers Digital Audio tape quality sound, allowing the receiver to directly feed a consumer's personal DAT machine. SkyPix intends to add a number of music-only DAT-quality entertainment channels.

Perhaps the best future-proof feature of the SkyPix receiver is its standard RS-232 Serial Data Port: this oft-overloooked feature of the SkyPix receiver will allow consumers to download data and software to their own personal computers and peripherals. Fax newspapers on demand? Home game software delivery? The mind boggles. SkyPix will announce the formation of a data service for consumers shortly. 256 kilobit data streams, individually addressed or broadcast to multiple customers, are possible.

When more than two-dozen services were beaming down to SkyPix' demo in Las Vegas: the image became crystal clear: here is a consumer-friendly appliance whose digital audio, digital video, reprogrammability and data services delivery potential are robust enough to form the core of a digital video multimedia system. But, first SkyPix needs to get basic entertainment services on its data stream. Then, it can go tackle - or woo - Nintendo.

The revamped SkyPix receiver uses the same Compression Labs, Inc./Integrated Information Technology silicon video decompression as last year, but there have been improvements made in both the real-time video compression uplink and the microcode-programmable ITT processor

video decompression side.

The 1992 SkyPix picture has more detail, and less motion artifact, than the 1991 system. And, that bodes well that should the medium-power Ku-band SkyPix take off this spring, that additional improvements can beremote-programmed into the box; with no need to enter the consumer's home. The revised uplink facility in Oxford, CT can now deliver up to 80 channels.That will allow SkyPix customers to never be more than 30 minutes away from the start of a hit movie. The revised receiver also employs a consumer removable data cartridge, which houses the compression, encryption and video circuitry.

The company's confidence in the reliability of this scheme has led to the creation of a five year warranty on the system. The cost of that warranty has been bundled into the SkyPix receiver pricing, raising its suggested retail above $800. The company behind the new receiver design is Mitsubishi International Corp. It has agreed to finance and build the construction of SkyPix receivers. Sanjeet Saxena, former SkyPix project director while at Mitsubishi, has been hired on by SkyPix as its director of corporate affairs. "It really doesn't get more exciting than this.," said Saxena. "The concept, the project and the people involved with SkyPix are all top-flight. I'm looking forward to the challenge."

Communications and Computer Enginners Research New "Mixed-Media" Satellite-Deliverable Digital Video Services

The desire to make computer digital processing more compatible with a broad range of human communications capabilities is propelling a host of research groups to engineer better ways of meshing audiovisual information streams with established binary Boolean and parallel data processing schemes.

If successful, this research into the encoding, processing and delivery of mixed-data types may lead to a new interpersonal era of man and machine; consumers and appliances. And, the medium best suited to deliver it is satellite; as cable companies struggle to expand bandwidth and initiate digital delivery of compressed video channels and data, satellite is far closer to com-

DirecTv: Thomson/Hughes Reach for the Sky Cable in 1994

RCA has won the contract to design and build the eighteen-inch diameter DirecTv Ku-band dish which feeds a high-power DBS satellite signal directly to an MPEG++ 2.5 x 15 x 12-inch decoder box. Signal security is provided by a removable security card system engineered by London-based News Datacom, which has an unbroken record of security in European DBS service.

The $700 (retail) system would be delivered in 24 months, after a December 1993 launch. Four live video feeds or eight movie channels can be compressed on each transponder in real time. In all, each fixed dish antenna would be capable of receiving a combination of 100 channels of compressed video and HDTV feeds from sixteen 120 watt transponders; should Thomson and the ATRC win their HDTV contract competition. RCA beat out General instrument, Scientific-Atlanta, AT&T, JVC and others in securing the Hughes DirecTv bid. RCA has an eighteen month (or one million receiver) exclusive with Hughes before licensing of the technology to other dish and receiver makers commences.

Thomson says MPEG++ data rates between 4 and 7 MBits/second will support DirecTv or Digital Cable delivery of 16:9 digital TV programming. HDTV requires 24 MBits/sec. Donahue: "We are dedicated to testing the industry to use world standards (such as MPEG)." Thomson declined to be specific about what interconnectivity options the box would have should Thomson and the ATRC lose the U.S. HDTV testing bid.

mercial implementation.

There are nearly four-million TVRO systems which can be easily upgraded to digital video and data services delivery. Unweaving this tapestry of parallel mixed-data delivery threads is a hot topic at dozens of corporate, university and government research labs around the globe. Their quest is to establish data architectures which will enable people to review audiovisual data material with the same digital ease as computer graphics and ASCII text files are now entered, scanned, accessed, modified and reviewed.

Engineers are finding that it is far more important to maintain a continuous stream of voice and/or music than it is to maintain a continuous video data rate. In other words, video doesn't have to be a steady 30 frames per second. For example, while human factors engineers have discovered that people prefer motion to be at a bare -minimum near film projection rates (24 frames per second) video can be enhanced up through to fifty and 60 frames (or fields per second).

But, because commercial computers vary in and are limited by their individual processing power, mixed media designers are working to develop platform-independent means of data storage and retrieval. For example, a workstration user might be able to retrieve digitized audiovisual materials at their full original frame rate. But, a desktop PC user, possessing less processing power, might have to be content to having just continuous audio playback with video displayed at a reduced fame rate, perhaps eight frames per second. But the other satellite system imperative concerning designers of these next generation satellite-delivered alternatives to cable is the transparent mixing of data and video for security purposes, ensuring broad, economical distribution.

The secure data bus of a computer audiovisual platform is a far cry from the additional error-correction, detection and correction data enhancements needed to support the transmission of these data types over long distance media: Local Area Networks, telephone lines, fiber optic lines, satellite and radio broadcast systems are feasible candidates, but none has the signal bandwdith breadth of satellite delivery. And, digital technology will allow satellite uplinkers to trade off the amount of bandwdith, and bandwdith-hungry data correction overhead, needed for mixed-signal satellite delivery.

Media data bandwidth minimization is a secondary concern to mixed-data researchers. And, because different types of information require different degrees of data integrity, engineers are evaluating digital encoding tradeoffs that have a parallel in the analog world of signal to noise ratio and 'static.'

For example, it is largely accepted that there is a lesser need for high error correction data overhead for stored images than for digitized music. Humans tend to use their eye-brain combination to ignore "static" or snow in a picture better than they tolerate noise or static in a section of music; or a table of numbrs or ASCII text errors.

The advances researchers are looking forward to as their experiments proceeed include the ability to slow down and speed-up human speech without the annoying "Daffy Duck" effect which accompanies analog processing, and grant capability for digitized video to be shown across a variety of playback platforms at a various speeds, resolutions and frame rates.

A new form of computer architecture parallism is presenting broad technology challenges to engineers, as companies, educational institutions and government researchers race to develop mixed-media data control architectures. The core of these teams research involves evaluating two trunks of mixed media research.

The first involves interleaving; mixing together threads of binary data, digitized voice, sound, video and graphics data. This then allows a variety of un-weaving architectures to process as much (or as little) of each data type as needed. The common denominator here is a solid temporal realtionship: each parallel, interwoven thread has an instantaneous time relatonship to all others. In this sense, it is a digital mixed-media

approach to the Frequency Modulation and Amplitude Modulation schemes long used for the RF transmission of audio, video and data. But, using digital coding and parallel interleaving of all data types, digital interleaving portends to be much more efficient, spectrally, than existing analog AM, FM and FSK systems.

The alternative method is using data buffering of each data type. This adds an aditional processing step (and data overhead) and the need to time-tag each data type, for later reassembly. Its primary appeal at present is that it is more amenable to single-processsor audiovisual systems, such as desktop PCs.

In between these two camps, MIT researchers are racing to complete and define a so-called open archiectrure for digital mixed media. A definition which may support satellite applications as far ranging as remote medical diagnosis (teleradiology diagnosis of x-ray images) to HDTV broadcasting to interplanetary image transmission from space probes.

The innovations section is contributed by Kyra Communications located in Seaford, NY at (516) 783-6244.

ANALYSIS

Compressed Digital Broadcast Video Technology:

Adoption Potential Among Business Television Networks

(Summary of a comprehensive study printed by KJH Communications, June 20, 1991)

USER AWARENESS AND PERCEPTIONS OF QUALITY

All network managers were familiar with technology development in the area of compressed digital video technology, but only six had seen actual over-the-air demonstrations or laboratory simulations.

Nevertheless over 70 percent thought a data rate ranging from 3 to 18 Mbps would be acceptable for at least some of the programs aired on their network. The remainder either cited concerns about the video quality at those data rates or had not yet reached an opinion.

For those with positive perceptions, the amount of programming for which a digital signal likely would be acceptable ranged from 20 percent to 100 percent of programs aired. Most-mentioned applications for private networks included management communications, training, and product introductions.

PROPOSED ADVANTAGES VS. USER NEEDS AND MARKET REALITY

Vendors and other advocates of compressed digital technology suggest that it will increase the number of business television networks and the amount of business television programming by offering -

- more available satellite capacity
- less expensive transmission channels
- an opportunity for users to produce multiple channels of programming

While these promises are on the surface extremely attractive, we offer the following comments to put them in a business perspective:

Availability

In the last two years, satellite capacity has been more difficult to obtain, particularly for occasional-use applications. While the prospect of using a portion of a transponder rather than a whole transponder suggests increased availability of capacity and reduced prices, to date none of the satellite operators or third-party suppliers have introduced an offering or a tariff for such business television services.

Cost

We feel certain that sales and operational concerns of the satellite operators will lead to relative price increases, not decreases. For example, one-eighth of a transponder will not be provided at one-eighth of the full transponder price. One-half of the price is a more realistic estimate.

Given the cost of replacing analog ground segment with digital, many existing networks will be hard pressed to receive a return on investment in a reasonable time for converting from analog to digital. Depending on network size and hours of broadcasting (and assuming that analog equipment is fully depreciated), our analysis shows that payback periods to break even range from a few months to over four years. Best cases are where network size is small and hours of programming are high.

For potential new private networks, a digital installation rather than an analog installation will improve the business case by less than 5 percent, based on a 50 percent savings of satellite time, which accounts for less than 10 percent of total operating and capital costs of most networks over a 5-year network life. The digital advantage will rarely be sufficient to justify a network that was unable to be justified in an analog scenario. We therefore question vendor predictions of a substantial increase in numbers of new networks because of digital technology.

Multiple Channels

Today, of approximately one hundred U.S. users of private and program business television networks, only 5 percent operate more than one simultaneous channel of programming. Nevertheless, 50 percent of the networks in the survey indicate a desire to operate multiple channels simultaneously. This does not necessarily mean day-long programming. In some cases multiple channels would mean merely the ability to purchase two 15-minute blocks of satellite time for the occasional broadcast of short programs to two different audience segments at the same time. Overall, the requirements for multiple simultaneous channels among private networks ranged from 2 to 8 channels, primarily at under 10 hours per week. For program/-educational networks, there are requirements for 2 to 12 channels ranging from 10 hours per week to 24 hours per day.

Given the tremendous resources required to produce business television programming and the as-yet lack of service offerings for occasional short blocks of time, we believe that less than half of the requirements articulated in this survey are likely to be implemented in the first two years of a digital environment.

An exception is the education network where production consists primarily of the transmission of a live class with limited production value and cost. For this reason, an educational network is among the first to adopt digital broadcast technology, and the prospect of other "universities of the air" has widespread appeal.

LIKELY ADOPTION SCENARIOS

Based on our assessment of the products and the marketplace, and assuming that compressed digital equipment prices are comparable to current analog B-MAC prices, we believe that most new networks will be implemented in digital format beginning in 1992 when the products are ready for delivery in quantity to the marketplace. The chief drivers for this choice will be the perception that digital technology is state-of-the-art compared to analog technology and the desire to position the network for future digital transmission developments.

Among existing networks, there will be conversion from analog to digital transmission where network size is small, satellite time is great, and/or multiple channels are required.

The Analysis section is contributed by KJH Communications located in Atlanta, Georgia at (404) 432-0625.

c

DECTEC INTERNATIONAL INC.

P.O. BOX 2275, 1962 MILL ROAD, STONEY [illegible] COLUMBIA, CANADA V8L 3S8
PHONE: (604) 655-4463 FAX: (604) 655-3906

PRESS RELEASE

DATE: 9 May 1991

TITLE: S.U.N.: Expert Third Party Patent Analysis (doc.2)

SUBJECT: Summaries of options as to whether or not DECTEC's S.U.N. scrambling system infringes patents owned by Cable/Home Communications Corp. (a wholly owned subsidiary of General Instrument Corp.) and M.A. Com Linkabit Inc. (also Titan Linkabit Corp.)

FROM: John Grayson

Filed Thursday 4 April 1991, by Harry L. Tredennick, Ph.D., P.E., President, Tredennick Inc. (Tredennick is an engineering firm specializing in the analysis of advanced digital electronics):

> "It is my opinion as a Registered Professional Engineer that the DECTEC International S.U.N. descrambling system and the associated Smart Card neither used nor needs to use any subscriber key seed signal that is unique to the descrambler (as described in General Instrument's Canadian patent . . . and the equivalent U.S. patent which carries the same title) to perform its descrambling function for Videocipher II - compatible transmissions . . ."

Filed 22 April 1991, by David V. Carlson, an attorney with the patent law firm Seed & Berry:

> "We have received the . . . (General Instrument) . . . patents and their claims and compared the proposed DECTEC descrambler as described above to the claims. We have also studied the file wrappers and relevant prior art cited against these patents. Our opinion is based on the above description of the DECTEC descrambler, the prior art, and file wrappers of relevant patents. As explained below, it is our opinion that the proposed DECTEC International S.U.N. descrambling system does not infringe any claim of the . . . (General Instrument) . . . patents, either literally or under the doctrine of equivalents."

Tredennick
4340 Stevens Creek Blvd., Suite 205
San Jose, CA 95129-1102
408 241-8790 (408 244-5435 fax)

ORIGINAL

Thu, 4 Apr, 1991

Mr. John Grayson
CEO
DECTEC International Inc.
P.O. Box 2275
Sidney, British Columbia
V8L3S8 Canada

Dear Mr. Grayson:

It is my opinion as a Registered Professional Engineer (Texas , USA, #44328) that the Dectec International SUN descrambling system and the associated Smart Card neither uses nor needs to use any "subscriber key seed signal that is unique to the descrambler" (as defined in General Instrument's Canadian patent #1225458 "Descrambler Subscriber Key Production System Utilizing Key Seeds Stored in Descrambler" and the equivalent U.S. patent which carries the same title—U.S. patent #4,634,808) to perform its descrambling function for VideoCipher II-compatible transmissions. I base my opinion on the work of Jeff Zimmer, an electrical engineer working for Tredennick, Inc., who studied the Dectec International SUN descrambling system while working under my direct supervision. Jeff's work included examination of the hardware and a line by line examination of the relevant software along with assembly and verification of code function.

Sincerely,

Harry L. Tredennick, Ph.D., P.E.
President, Tredennick, Inc.
Texas, USA P.E. # 44328

LAW OFFICES
SEED AND BERRY
6300 COLUMBIA CENTER
701 FIFTH AVENUE
SEATTLE, WASHINGTON 98104-7092
(206) 622 4900

TELEX: 3723836 SEEDANBERRY
FAX, II-III: (206) 682-6031

PATENT, TRADEMARK, COPYRIGHT, UNFAIR COMPETITION
COMPUTER LAW, BIOTECHNOLOGY LAW AND RELATED
LITIGATION AND LICENSING

ROBERT J. BAYNHAM
EDWARD W. BULCHIS
DAVID H. DEITS
WILLIAM O. FERRON, JR.
DAVID J. MAKI
PAUL T. MEIKLEJOHN
GEORGE C. RONDEAU, JR.
RICHARD W. SEED

BENJAMIN T. BERRY
(1918-1988)

DAVID V. CARLSON
I. GRANT FOSTER
GEORGE B. FOX
KARL R. HERMANNS
JOHN M. KELLY
DAVID D. McMASTERS
MAURICE J. PIRIO
JONATHAN R. RAPPAPORT
RICHARD G. SHARKEY
FRANCES G. SMITH
ROBERT M. STORWICK
KENNETH G. WHITAKER

April 23, 1991

Mr. John Grayson, C.E.O.
DECTEC INTERNATIONAL, INC.
P.O. Box 2275
1962 Mills Road
Sidney, British Columbia V8L 3S8
Canada

Our Reference: 250050.001

Dear Mr. Grayson:

You have requested that we provide an opinion as to whether or not the Dectec descrambling system as currently proposed infringes the following three U.S. patents: Gilhousen et al., U.S. Patent No. 4,613,901 ('901); Moerder, U.S. Patent No. 4,634,808 ('808); and Paik et al., U.S. Patent No. 4,608,456 ('456). A computer database listing the ownership of U.S. patents indicate that a one-half interest in the patents was assigned to Cable/Home Communication Corp. of San Diego, California in September of 1987 (a wholly owned subsidiary of General Instrument) and that M/A Com Linkabit, Inc. changed their name to Titan Linkabit Corp. in September of 1990.

The Dectec descrambling system proposed for sale in the U.S. includes a Smart Card containing nonvolatile SRAMS in a credit card-sized package. The Smart Card is custom manufactured by Dallas Semiconductor and a custom software program stored therein according to Dectec's specifications. Six Xilinx software programmable gate array chips within the descrambler are addressable by the Smart Card. A program is downloaded from the Smart Card into the software programmable gate array chips to configure them as hardware logic that can descramble the combined video and audio signal that has been encrypted by the VideoCipher II standard.